О. И. Шелухин, Д. Ж. Сакалема, А. С. Филинова

ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ В КОМПЬЮТЕРНЫЕ СЕТИ

[сетевые аномалии]

Под редакцией профессора О. И. Шелухина

Рекомендовано УМО по образованию в области Инфокоммуникационных технологий и систем связи в качестве учебного пособия для студентов высших учебныз заведений, обучающихся по направлению подготовки 210700 - «Инфокоммуникационные технологии и системы связи» квалификации (степени) «бакалавр» и «магистр»

Москва
Горячая линия - Телеком
2013

Электронный архив библиотеки МТУСИ

УДК 004.732.056(075.8)
ББК 32.973.2-018.2я73
Ш44

Р е ц е н з е н т ы : доктор техн. наук, профессор, академик РАЕН, декан факультета «Кибернетика и информационная безопасность НИЯУ МИФИ» *С. В. Дворянкин*; доктор техн. наук, профессор, зав. кафедрой «Информационная безопасность телекоммуникационных систем» ЮФУ *К. Е. Румянцев*; доктор техн. наук, профессор кафедры «Информационная безопасность и автоматизация» МТУСИ *С. С. Звежинский*; канд. техн. наук, доцент кафедры «Информационная безопасность» МГТУ им Н. Э. Баумана *Р. А. Бельфер*;

Шелухин О. И., Сакалема Д. Ж., Филинова А. С.

Ш44 Обнаружение вторжений в компьютерные сети (сетевые аномалии). Учебное пособие для вузов. / Под ред. профессора О. И. Шелухина – М.: Горячая линия–Телеком, 2013. – 220 с: ил.

ISBN 978-5-9912-0323-4.

Даны основные определения и понятия в области систем обнаружения вторжений и компьютерных атак. Рассмотрены принципы построения и структура систем обнаружения вторжений. Анализируются способы развертывания, достоинства и недостатки существующих систем обнаружения вторжений. Центральное место в книге уделено методам обнаружения сетевых аномалий. Рассмотрены методы кратномасштабного вейвлет- и мультифрактального анализа алгоритмов обнаружения аномальных вторжений. Проведен анализ статистических, интеллектуальных, иммунных, нейросетевых и других алгоритмов обнаружения аномалий.

Для студентов, обучающихся по направлению подготовки бакалавров и магистров 210700 – «Инфокоммуникационные технологии и системы связи», может быть полезно аспирантам и студентам, обучающимся по группе специальностей направления «Информационная безопасность» и специалистам в области защиты информации и безопасности инфокоммуникаций.

ББК 32.973.2-018.2я73

Учебное издание

Шелухин Олег Иванович, **Сакалема** Домингуш Жайме,
Филинова Анастасия Сергеевна

Обнаружение вторжений в компьютерные сети (сетевые аномалии)
Учебное пособие для вузов

Редактор Ю. Н. Чернышов
Компьютерная верстка Ю. Н. Чернышова
Обложка художника О. Г. Карповой

Подписано к печати 07.02.2013. Формат 60×88 1/16. Усл. печ. л. 13,75. Изд. № 13323. Тираж 500 экз. (1-й завод 200 экз.)

ISBN 978-5-9912-0323-4

ПРЕДИСЛОВИЕ

Важнейшим атрибутом нашего времени является глобальная информационная интеграция, основанная на построении компьютерных сетей масштаба предприятия и их объединении посредством Интернета.

Сложность логической и физической организации современных сетей приводит к объективным трудностям при решении вопросов управления и защиты сетей. В процессе эксплуатации компьютерных сетей администраторам приходится решать две главные задачи:

- диагностировать работу сети и подключенных к ней серверов, рабочих станций и соответствующего программного обеспечения;
- защищать информационные ресурсы сети от несанкционированной деятельности хакеров, воздействий вирусов, сетевых червей и т. п., т. е. обеспечивать их конфиденциальность, целостность и доступность.

При решении задач, связанных с диагностикой и защитой сетевых ресурсов, центральным вопросом является оперативное обнаружение состояний сети, приводящих к потере полной или частичной ее работоспособности, уничтожению, искажению или утечке информации, являющихся следствием отказов, сбоев случайного характера или результатом получения злоумышленником несанкционированного доступа к сетевым ресурсам, проникновения сетевых червей, вирусов и других угроз информационной безопасности. Раннее обнаружение таких состояний позволит своевременно устранить их причину, а также предотвратит возможные катастрофические последствия.

Для их обнаружения используется большой спектр специализированных систем. Так, при решении проблем диагностики сетей применяются средства систем управления, анализаторы сетевых протоколов, системы нагрузочного тестирования, системы сетевого мониторинга. Проблемы защиты информационных ресурсов сетей решаются с помощью межсетевых экранов (firewall), антивирусов, систем обнаружения атак (СОВ) (Intrusion Detection System, IDS), систем контроля целостности, криптографических средств защиты.

Характерными особенностями использования этих систем является либо их периодическое и кратковременное применение для решения определенной проблемы, либо постоянное использование, но со статическими настройками. В результате методы анализа, используемые в современных системах, направлены на обнаружение известных и точно описанных типов воздействий, но зачастую оказываются не в состоянии обнаружить их модификации или новые типы, что делает их использование малоэффективным.

Таким образом, на сегодняшний день очень актуальной задачей является поиск более эффективных методов выявления недопустимых событий (аномалий) в работе сети, являющихся следствием технических сбоев или несанкционированных воздействий. Основным требованием к этим методам является возможность обнаружения произвольных типов аномалий, в том числе новых, а также воздействий, распределенных во времени.

Это направление научных исследований является очень молодым. Первые работы, посвященные данной проблеме, были опубликованы в 90-х годах прошлого столетия.

В настоящий момент исследования в этой области ведутся крупными зарубежными коммерческими компаниями. Общий подход, лежащий в основе этих исследований, заключается в поиске методов анализа, позволяющих выявлять аномальные состояния информационных ресурсов в виде отклонений от обычного («нормального») состояния. Эти отклонения могут являться результатами сбоев в работе аппаратного и программного обеспечения, а также следствиями сетевых атак хакеров. Такой подход теоретически позволит обнаруживать как известные, так и новые типы проблем. От эффективности и точности аппарата, определяющего «нормальное» состояние и фиксирующего отклонение, зависит в целом эффективность решения вопросов диагностики и защиты сетевых ресурсов. Особую важность на текущий момент представляет проблема обнаружения аномальных состояний в работе сети, имеющих распределенный во времени характер (АРВ). АРВ могут являться следствиями специально маскируемых сетевых атак злоумышленников, скрытых аппаратно-программных сбоев, новых вирусов и т. п.

В основу учебного пособия положен курс лекционных, практических и лабораторных занятий для студентов МТУСИ, обучающихся по магистерским программам «Программно-защищенные инфокоммуникации» в рамках направлений «Инфокоммуникационные технологии и системы связи», а также «Информатика и вычислительная техника».

Оглавление